Claims

What is claimed is:

(1) Method for the secure and controlled loading of applications onto a conventional file system smart card without the benefit of card based cryptographic services or a virtual machine such as Java.

(2) Method of claim 1 further consisting of a plurality of single use key files which have been initially written to the smart card by the card issuer and which values may, in turn, be selectively disclosed to third parties in order to grant access for application loading.

(3) Method of claim 2 wherein the key file values are rendered unusable after first use thereby restricting these as one time only keys.

(4) Method of claim 1 further consisting of a plurality of smart card files (each protected by its associated key file as described in claim 2) in which the currently active master key value (“card unlock key” for short) needed to unlock the card is stored.

(5) Method of claim 4 wherein the “card unlock key” value is randomly generated after each use and is therefore different for each card and each session.

(6) Method of claim 1 further consisting of a second “card unlock key” known only to the card issuer which could override any other card operations thereby allowing specific applications to be deactivated.

(7) Method of claim 1 wherein the said application loading can take place even after the card has been placed into circulation.

(8) Method of claim 1 wherein the said application loading is dynamic thereby affording greater flexibility than attempting to fit applications into a predefined card template.

(9) Method of claim 1 to also include the unloading of applications.

(10) Method and system for the Card Issuer to selectively empower third parties to be able to load applications to the smart card.

(11) Method of claim 10 further consisting of a secure process for individually authorizing and controlling application loading.

(12) Method of claim 10 wherein the authorization can be granted after the card has been placed in circulation.

(13) Method of claim 10 wherein the Card Issuer maintains a reversionary ownership interest in the card such that applications can be inactivated or removed.

(14) Method and system to logically separate the smart card memory such that partitioned applications cannot corrupt of otherwise interfere with each other.

(15) Method of claim 14 wherein partitioned card memory is only available to authorized application providers and cannot be accessed through unlicensed means.

(16) Method of claim 14 wherein application providers can create security schemes local to their authorized application directory thereby controlling access to data within that application directory.